A NOTE ON ZEROS OF L-SERIES OF ELLIPTIC CURVES

Xian-Jin Li

Abstract. In this note we study an analogy between a positive definite quadratic form for elliptic curves over finite fields and a positive definite quadratic form for elliptic curves over the rational number field. A question is posed of which an affirmative answer would imply the analogue of the Riemann hypothesis for elliptic curves over the rational number field.

1. Introduction. In the last entry of his diary, Gauss had noted the number N of integer solutions of the congruence

$$x^2y^2 + x^2 + y^2 \equiv 1 \mod p$$

for a prime number $p \equiv 1(\mod 4)$ is given by the formula

$$N = p + 1 - (\pi + \bar{\pi}),$$

where π is defined by the decomposition $p = \pi\bar{\pi}$ in the ring $\mathbb{Z}[i]$. It follows that

$$|p + 1 - N| \leq 2\sqrt{p}.$$

Gauss did not give a proof for his statement. In 1921 [7], G. Herglotz presented a proof of Gauss' statement using complex multiplication.

In 1933 H. Hasse [5] [6] used complex multiplication, which is in essence the same method that G. Herglotz used, to prove the analogue of the Riemann hypothesis for all elliptic function fields. Let $\mathbb{F}_q$ be a finite field with q elements, and let E be an elliptic curve over $\mathbb{F}_q$. H. Hasse proved the inequality

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}, \tag{1.1}$$

where $\#E(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points of the elliptic curve.

In his book [4], H. Hasse said: "The analogous procedure for the ordinary RH in algebraic number fields would be to get a best possible estimate of the prime number function $\Pi(x)$ or rather its analogue for prime divisors in algebraic number fields. From Riemann's exact formula one can deduce that an estimate with error term $O(\sqrt{x})$ or only $O(\sqrt{x}\log x)$ would establish RH. Nobody however has been trying this most natural approach to the ordinary RH up to now!"

1991 *Mathematics Subject Classification.* Primary 11M26.

Key words and phrases. Artin's product formula, Cauchy-Schwartz' inequality, height pairing.

Research supported by National Security Agency H98230-06-1-0061

Although the author does not understand the statement above, he feels that it may indicate a method to attack the analogue of the Riemann hypothesis for elliptic curves over the rational number field, which is the content of this note.

We briefly review a proof of Hasse's inequality (1.1) in section 2. In section 3, an analogous procedure is presented for elliptic curves over the rational number field. A question is posed of which an affirmative answer would imply the analogue of the Riemann hypothesis for elliptic curves over the rational number field.

This note was initiated at the Workshop on Zeta-Functions and Associated Riemann Hypotheses, New York University, Manhattan, May 29 - June 1, 2002. He wants to thank the American Institute of Mathematics, Brian Conrey, and Peter Sarnak for the financial support for him to attend the workshop.

2. L-series of elliptic curves over finite fields. Let A be an abelian group. A function $d : A \to \mathbb{R}$ is called a positive definite quadratic form if $d(\alpha) = d(-\alpha) \geq 0$ for all $\alpha \in A$ with equality if and only if $\alpha = 0$, and if the pairing

$$\langle \alpha, \beta \rangle = d(\alpha + \beta) - d(\alpha) - d(\beta)$$

is bilinear on A. The degree map $\deg : \mathrm{Hom}(E, E) \to \mathbb{Z}$ is a positive definite quadratic form; see [10]. Denote

$$\langle \psi, \phi \rangle = \deg(\psi + \phi) - \deg(\psi) - \deg(\phi).$$

Since $\langle m\psi + n\phi, m\psi + n\phi \rangle \geq 0$ for all integers m and n, we have the Cauchy-Schwartz inequality

$$|\deg(\psi - \phi) - \deg \psi - \deg \phi| \leq 2\sqrt{\deg \psi \deg \phi} \tag{2.1}$$

for all morphisms $\psi, \phi \in \mathrm{Hom}(E, E)$. Let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a Weierstrass equation for E with coefficients in $\mathbb{F}_q$. If

$$\phi : E \to E, \ (x, y) \to (x^q, y^q)$$

denotes the q^{th}-power Frobenius morphism of E, then $\deg \phi = q$ and

$$\deg(1 - \phi) = \#E(\mathbb{F}_q).$$

Thus, Hasse's inequality (1.1) follows from (2.1); see [10].

Let $a = q + 1 - \#E(\mathbb{F}_q)$. The L-series of the elliptic curve E over $\mathbb{F}_q$ is given by

$$L_E(s) = 1 - aq^{-s} + q^{1-2s}.$$

By Hasse's inequality we have

$$L_E(s) = (1 - \alpha q^{-s})(1 - \beta q^{-s})$$

with $\bar{\alpha} = \beta$ and $|\alpha| = |\beta| = \sqrt{q}$. Hence, the analogue of the Riemann hypothesis for L-series of elliptic curves over finite fields follows from the Cauchy-Schwartz inequality (2.1).

3. L-series of elliptic curves over $\mathbb{Q}$. Let E be an elliptic curve over the rational number field $\mathbb{Q}$, and let $\hat{h}$ the canonical height on E. By Artin's product formula, we have

$$\hat{h}(P) \geq 0$$

for all points $P \in E(\bar{\mathbb{Q}})$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in the complex numbers. The Néron-Tate pairing on E is the bilinear form

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

for all points $P, Q \in E(\bar{\mathbb{Q}})$; see [10]. Since $\langle mP+nQ, mP+nQ\rangle \geq 0$ for all integers m and n, we have the Cauchy-Schwartz inequality

$$|\hat{h}(P-Q) - \hat{h}(P) - \hat{h}(Q)| \leq 2\sqrt{\hat{h}(P)\hat{h}(Q)} \tag{3.1}$$

for all points $P, Q \in E(\bar{\mathbb{Q}})$. Note that the fundamental theorem of arithmetic is implicitly used in (3.1) because of Artin's product formula.

Let N be the conductor of E. For each prime p, we denote the reduction of E at p by $\tilde{E}_p$. Let

$$a_p = \begin{cases} p+1-\#\tilde{E}_p(\mathbb{F}_p), & \text{if } E \text{ has good reduction at } p \\ 1, & \text{if } E \text{ has split multiplicative reduction at } p \\ -1, & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 0, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

The L-series associated to the elliptic curve E is defined by the Euler product:

$$L_E(s) = \prod_{p\nmid N}(1-a_p p^{-s}+p^{1-2s})^{-1}\prod_{p|N}(1-a_p p^{-s})^{-1}$$

for $\Re s > 3/2$.

By results in [3] [9] and the Shimura-Taniyama conjecture that is a theorem proved in [2] [11], there is a normalized Hecke eigenform f of weight 2 and level N and of rational Fourier coefficients such that $L_f = L_E$. Hence $L_E(s)$ has an analytic continuation to the complex plane and satisfies the functional equation

$$\Gamma(s)L_E(s) = wN^{1-s}(2\pi)^{2s-2}\Gamma(2-s)L_E(2-s),$$

where $w = (-1)^r$ with r being the vanishing order of $\xi_f(s)$ at $s = 1/2$; see [1].

Let

$$\xi_E(s) = N^{s/2}(2\pi)^{-s}\Gamma(\frac{1}{2}+s)L_E(\frac{1}{2}+s).$$

Then $\xi_E(s)$ is an entire function and satisfies the functional identity

$$\xi_E(s) = w\xi_E(1-s).$$

Let $\varphi(z) = \xi_E(1/(1-z))$, and let

$$\frac{\varphi'(z)}{\varphi(z)} = \sum_{n=0}^{\infty}\lambda_E(n+1)z^n. \tag{3.2}$$

Similarly as in [8], we can show that all zeros of $\xi_E(s)$ lie on the line $\Re s = 1/2$ if and only if $\lambda_E(n) \geq 0$ for $n = 1, 2, \cdots$.

On the other hand, to show that all zeros of $\xi_E(s)$ lie on the line $\Re s = 1/2$ it suffices to obtain upper bounds for the $\lambda_E(n)$'s that would give the convergence of the series (3.2) for $|z| < 1$. Studying H. Hasse's proof of the Riemann hypothesis for elliptic curves over finite fields leads the author to believe that the following question should have an affirmative answer.

Question. *Is it possible that there exist points $P, Q \in E$ such that certain upper bounds for the $\lambda_E(n)$'s, which would give the convergence of the series (3.2) in the unit disk $|z| < 1$, can be obtained by using the Cauchy-Schwartz inequality (3.1)?*

References

1. A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann. **185** (1970), 134–160.
2. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
3. H. Carayol, *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. **19** (1986), 409–468.
4. H. Hasse, *The Riemann Hypothesis in Algebraic Function Fields over a finite constants field*, Pennsylvania State University, University Park, 1968.
5. H. Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufige Mitteilung*, in "Helmut Hasse Mathematische Abhandlungen," Band 2, deGruyter, 1975, 85–94.
6. H. Hasse, *Modular functions and elliptic curves over finite fields*, in "Helmut Hasse Mathematische Abhandlungen," Band 2, deGruyter, 1975, 351–369.
7. G. Herglotz, *Zur letzten Eintragung im Gausschen Tagebuch*, Ber. Verhandl. Sächs. Akad. Wiss. Math.-Phys. Kl. **73** (1921), 271–276.
8. Xian-Jin Li, *The positivity of a sequence of numbers and the Riemann hypothesis*, J. Number Theory **65** (1997), 325–333.
9. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.
10. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
11. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443–551.

Department of Mathematics, Brigham Young University, Provo, Utah 84602 USA
E-mail address: xianjin@math.byu.edu